Listing and Amendments to the Claims

This listing of claims will replace the claims that were published in the PCT Application and annexed to the International Preliminary Report on Patentability:

1. (original) A method for controlling access to a network, said method comprising:

receiving, by an access point (AP) of said network, a request to access said network, said request transmitted by a client;

re-directing, by said AP, said access request to a local server;

associating unique data with an identifier of said client and storing a mapping of said association in said AP;

generating a Web page by said local server requesting that said client select an authentication server (AS) and including said unique data and forwarding said generated Web page to said client;

transmitting an authentication request to said selected authentication server; and

receiving a response to said authentication request from said selected authentication server.

2. (original) The method according to claim 1, wherein said network is a wireless Local Area network (WLAN).

3. (original) The method according to claim 1, further comprising:

forwarding said identifier of said client from said local server; and

generating said unique data for said client by said local server.

4. (original) The method according to claim 1, further comprising:

retrieving, by said client, a re-directed URL having embedded data including a first digital signature, authentication parameters and said unique data and forwarding said re-directed URL to said AP;

creating, by said AP, a second digital signature using said authentication parameters, said unique data and said identifier;

comparing, by said AP, said first digital signature with said second digital signature;

determining, by said AP, if there is a match between said first digital signature and said second digital signature; and

performing, by said AP, one of granting network access and denying network access based on said match determination.

5. (original) The method according to claim 1, wherein said unique data includes a session ID and a randomized number.

6. (original) The method according to claim 1, wherein said identifier is an address of said client.

7. (original) The method according to claim 1, wherein the act of authenticating further comprises:

processing, by said AS, said authentication request, wherein said authentication request includes a session ID embedded in said authentication request;

responding to said authentication request by forwarding to said client by said AS an authentication input page, said authentication input page including a request for authentication information; and

receiving, by said AS, authentication credentials from said client, wherein said response to said authentication request forwarded to said client includes a re-direct header and a success code and associated information relevant to access of said network by said client.

8. (original) The method according to claim 7, wherein the act of forwarding further comprises generating, by said AS, said success code and said associated information includes a first digital signature and authentication parameters.

9. (original) The method according to claim 5, wherein said randomized number is one of a random number and a pseudo-random number.

10. (original) The method according to claim 1, wherein said identifier is one of a physical (PHY) address of said client, a MAC address of said client and an IP address of said client.

11. (original) The method according to claim 1, wherein said AP and said local server are co-located.

12. (original) The method according to claim 4, wherein said first and said second digital signatures are generated using one of a private key of said AS and a shared key between said AS and said local server.

13. (original) The method according to claim 4, wherein said second digital signature is locally generated at said AP.

Claim 14. (CANCELLED)

Claim 15. (CANCELLED)

Claim 16. (CANCELLED)

Claim 17. (CANCELLED)

Claim 18. (CANCELLED)

Claim 19. (CANCELLED)

Claim 20. (CANCELLED)

Claim 21. (CANCELLED)

Claim 22. (CANCELLED)

Claim 23. (CANCELLED)

Claim 24. (CANCELLED)

25. (original) A system for controlling access to a network comprising:

a client;

an access point (AP) coupled to a local server (LS) for relaying network communications to and from the client; and

an authentication server for performing an authentication process in response to a request from the client; wherein

the AP, in response to a re-directed request to access the network from the client, associates unique data with an identifier of the client and stores a mapping of the association;

the LS transmits the unique data to the client;

the authentication server, upon authenticating the client using the unique data, is operative to provide a re-direct header for access to the client including a digitally signed authentication message and authentication parameters corresponding to the unique data, the AP receiving the digitally signed retrieved re-directed URL and authentication parameters from the client and the AP further correlating the authentication parameters with the mapped association data for determining access to the network based on the results of the correlation.

26. (original) The system of claim 25, wherein the network is a wireless local area network (WLAN) comprising the access point and local server.

27. (original) The system of claim 25, wherein the local server generates a web page requesting that the client select an authentication server, and embeds the unique data in the web page for transmission to the client.

28. (original) The system of claim 25, wherein the identifier of the client is one of a physical address, MAC address and an IP address, and wherein the unique data comprises a session ID and a randomized number.

29. (original) The system of claim 28, wherein the session ID and randomized number are generated by the local server.

30. (original) The system of claim 28, wherein the authentication server receives user credential information from the client and provides a digitally signed authentication message including an authentication parameters using said unique data through HTTPS to the client via said re-direct header to the client.

31. (original) The system of claim 30, wherein the AP, in response to receiving the digitally signed authentication message re-directed from the client including the authentication parameters and at least a portion of the unique data from the client, generates a local digital signature using the received portion of the unique data and the stored mapping data together with the authentication parameters, and compares the local digital signature with the digitally signed authentication message to determine network access by the client.

32. (original) The system of claim 25, wherein the re-direct header further comprises a means for re-directing a browser of the client to a URL on the network, and embedding in the URL said digitally signed authentication message, the authentication parameters and a portion of the unique data.

33. (original) The system of claim 26, wherein said AP and said LS are co-located.

34. (original) The method of Claim 1, further comprising:

at the authentication server, authenticating the client using the unique data, and forwarding said response to the client using a re-direct header, and including a digitally signed authentication message and authentication parameters corresponding to the unique data; and

the access point receiving from the client according to the re-direct header the digitally signed authentication message and authentication parameters and correlating the authentication parameters with the mapped association data for determining access to the network.

Claim 35. (CANCELLED)

36. (original) The method of Claim 1, wherein said unique data comprises a session ID and a randomized number and further comprising: receiving, by said AP, a re-directed request from the client and including a digitally signed authentication message, an authentication parameter list, and said session ID, the digitally signed authentication message being generated using the randomized number, said session ID and said authentication parameter list, by said selected authentication server associated with the client; and

correlating the received digitally signed authentication message with the re-directed request for access using the stored mapping data for controlling access by the client to the network.

Claim 37. (CANCELLED)

Claim 38. (CANCELLED)

Claim 39. (CANCELLED)

Claim 40. (CANCELLED)

41. (original) The method according to claim 36, wherein said AP and said LS are co-located.

42. (new) A method for controlling network access, said method comprising:

receiving a request for network access;

re-directing said request via a message;

receiving a client identifier and unique data;

associating said unique data and said client identifier;

receiving a re-directed universal resource locator included embedded information;

generating a local digital signature using said embedded information and said association between said unique data and said client identifier;

comparing said local digital signature with a digital signature received in said embedded information;

granting network access if said local digital signature matches said digital signature received in said embedded information; and

deny network access if said local digital signature does not match said digital signature received in said embedded information.

43. (new) The method according to claim 42, wherein said unique data comprises a session identifier and a random number.

44. (new) he method according to claim 42, wherein said embedded information further comprises a session identifier and authentication parameters.

45. (new) A system for controlling network access, comprising:

means for receiving a request for network access;

means for re-directing said request via a message;

means for receiving a client identifier and unique data;

means for associating said unique data and said client identifier;

means for receiving a re-directed universal resource locator included embedded information;

means for generating a local digital signature using said embedded information and said association between said unique data and said client identifier;

means for comparing said local digital signature with a digital signature received in said embedded information;

means for granting network access if said local digital signature matches said digital signature received in said embedded information; and

means for deny network access if said local digital signature does not match said digital signature received in said embedded information.

46.. (new) The system according to claim 45, wherein said unique data comprises a session identifier and a random number.

47. (new) The system according to claim 45, wherein said embedded information further comprises a session identifier and authentication parameters.

48. (new) A method for controlling network access, said method comprising:
receiving a re-directed request for network access via a message;
transmitting a client identifier and unique data; and
generating a web page including embedded data.

49. (new) The method according to claim 48, wherein said unique data comprises a session identifier and a random number.

50. (new) The method according to claim 48, wherein said embedded data comprises a session identifier, a random number and authentication server selection information.

51. (new) A system for controlling network access, comprising:
means for receiving a re-directed request for network access via a message;
means for transmitting a client identifier and unique data; and
means for generating a web page including embedded data.

52. (new) The system according to claim 51, wherein said unique data comprises a session identifier and a random number.

53. (new) The system according to claim 51, wherein said embedded data comprises a session identifier, a random number and authentication server selection information.

54. (new) A method for controlling network access, said method comprising:
receiving an authentication user input message;
transmitting authentication input page requesting authentication information;
receiving authentication credentials; and
transmitting an authentication message indicating one of success and failure of an authentication process.

55. (new) The method according to claim 54, wherein said authentication message comprises a digital signature, a session identifier, authentication parameters and a random number.

56. (new) A system for controlling network access, comprising:

means for receiving an authentication user input message;

means for transmitting authentication input page requesting authentication information;

means for receiving authentication credentials; and

means for transmitting an authentication message indicating one of success and failure of an authentication process.

57. (new) The system according to claim 56, wherein said authentication message comprises a digital signature, a session identifier, authentication parameters and a random number.